Santa Clara Law Review

Volume 52 | Number 4 Article 12

12-23-2012

Electronic Discovery: The Challenges of Reaching Into the Cloud

Jacob Smith

ELECTRONIC DISCOVERY: THE CHALLENGES OF REACHING INTO THE CLOUD

Jacob Smith*

TABLE OF CONTENTS

INTRODUCTION

"Cloud computing," an amorphous and often misunderstood term, references an Internet-based methodology that service providers and web-based entities commonly use. The majority of Internet users unknowingly encounter cloud computing in their casual day-to-day web browsing. So-called "Web 2.0 applications," such as Gmail,

* B.S.E.E., Clemson University; J.D., Santa Clara University School of Law. I would like to thank my parents for their unwavering love and encouragement. And, special thanks to Christina Cheung for her boundless patience during the editing process.

Facebook, and LinkedIn, all utilize cloud computing. In a nutshell, all processing and data retention occurs away from the user's computer, in a cloud computing application at a service provider's remote location.

More and more companies are taking advantage of cloud computing services offered by providers such as Amazon, Google, Microsoft, and Yahoo!.[1] These cloud computing service providers allow companies to replace their expensive and aging technological infrastructure with third-party processing and storage capabilities that are accessible over the Internet.[2] Not only does this option save on overhead and infrastructure costs, but the cloud computing service providers also offer flexible pricing on a pay-for-use basis that offers attractive scalability.[3] This service permits easy access over the Internet or over a private network from any location, so that computer software and data may be readily available whenever and wherever.[4]

There are three basic types of cloud computing services: Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).[5] There are also four models for deployment of these services: private, public, community, and hybrid.[6] This Comment focuses exclusively upon private SaaS cloud services because they are the most commonly used type and model.

Private SaaS clouds permit access to a provider's software applications running on cloud infrastructure maintained for the benefit of a solitary enterprise.[7] The enterprise contracts with the provider to supply it with solutions to its particular business needs, such as data retention or remote database access. These solutions, contained entirely in the cloud, are considered private because the solutions are only accessible by the enterprise that is paying for the provider's services.

1. Mark L. Austrian & W. Michael Ryan, *Cloud Computing Meets E-Discovery*, CYBERSPACE LAW., July 2009, at 1.

2. *See id.*

3. W. Michael Ryan & Cristopher M. Loeffler, *Insights into Cloud Computing*, 22 INTELL. PROP. & TECH. L.J. 22, 22 (2010).

4. *Id.*

5. *See id.*

6. *See id.*

7. *See id.* at 22–23.

As more companies incorporate cloud computing into their day-to-day activities, their data accumulates in the cloud. Where this electronically stored information (ESI) goes, electronic discovery often soon follows.[8] A company that becomes involved in litigation may thereafter be required to produce some of the data that is stored in the cloud by the service provider.

Requests for the production of ESI can come in the form of a Rule 34 motion to compel production[9] or a Rule 45 subpoena directing a third-party service provider to produce ESI.[10] It would be prudent for companies to take preemptory measures to ensure that their third-party cloud computing service provider does not engage in spoliation, or the deletion, of ESI. Otherwise, a company involved in litigation may be subjected to sanctions for the deletion of ESI by its third-party service provider.[11]

Part I.A will address the Federal Rules of Civil Procedure (FRCP) applicable to electronic discovery.[12] Part I.B will discuss the application of the three elements of the *Zubulake IV* framework to ESI in the cloud, which provide a starting point for the mitigation of liability for discovery sanctions.[13] Finally, Part II will discuss how a company can reduce its liability by inserting protective electronic-discovery-specific provisions into the service agreement with its third-party cloud computing service provider.[14]

I. ELECTRONIC DISCOVERY IN THE CLOUD

With the relatively new introduction of electronic discovery procedures, by way of the 2006 Amendments to the FRCP, case law is still fleshing out and adapting the electronic discovery procedures with respect to today's

8. David D. Cross & Emily Kuwahara, *E-Discovery and Cloud Computing: Control of ESI in the Cloud*, EDDE J., Spring 2010, at 2.

9. FED. R. CIV. P. 34.

10. FED. R. CIV. P. 45.

11. *See, e.g.*, Bowman v. Am. Med. Sys., Inc., No. Civ. A. 96-7871, 1998 WL 721079, *4 (E.D. Penn. Oct. 9, 1998) (holding that a prosthetic implant production company was held liable for spoliation of evidence in a product liability suit even though such evidence was throw out by a third-party doctor).

12. *See infra* Part I.A.

13. *See infra* Part I.B.

14. *See infra* Part II.

technologies.[15] To add further uncertainty, companies are rapidly employing the use of third-party cloud computing data processing and retention services—an unexplored territory of jurisprudence.[16] Given the lack of jurisprudence in applying the electronic discovery rules to third parties, it is difficult to predict the outcome of electronic discovery disputes.

Parties involved in litigation may stretch to draw comparisons between past cases concerning tangible data held by third-parties and present scenarios where intangible data is held by a third-party cloud computing service provider.[17] But, the amount of administerial power held by the third-party cloud computing service provider over ESI is too dissimilar to draw a valid comparison.[18] For example, the third-party cloud computing service provider has more control than an average third-party maintaining paper copies of data, because the third-party cloud computing service provider is contracted to replace a company's existing data retention and processing infrastructure. In addition, the third-party cloud computing service provider may exercise its ability to alter or destroy the company's data subject to the service provider's routine deletion procedures.[19]

A. Federal Rules of Civil Procedure Applicable to Electronic Discovery

The 2006 Amendments[20] to the FRCP[21] paved the way for

15. *See* Cross & Kuwahara, *supra* note 8, at 3.

16. *See* Oregon v. Beller, 217 P.3d 1094, 1111 n.11 (Or. Ct. App. 2009) (Sercombe, J., dissenting). This is the only judicial opinion that expressly mentions cloud computing, and, even then, it is only mentioned in a footnote.

17. *See generally* Flagg v. City of Detroit, 252 F.R.D. 346, 354 (E.D. Mich. 2008); *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007); Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007).

18. *See* Cross & Kuwahara, *supra* note 8, at 5.

19. The safe harbor provision in Rule 37 may shield third parties from routine, good-faith deletion of ESI. FED. R. CIV. P. 37(e).

20. 2006 FRCP amendments applicable to this comment chiefly include those to Rules 26, 34, 37, and 45.

21. A discovery conference in 1996 first addressed the unique problems associated with the discovery of electronically stored information. Judicial Conf. of the U.S., Summary Rep. of the Comm. on the FED. R. CIV. P. app. C, at 18, *available at* http://www.uscourts.gov/rule/Reports/ST09-2005.pdf (last visited Mar. 15, 2011). After the Advisory Comm.'s comment, published Aug. 2004, and three public hearings the Advisory Comm. submitted their newly revised proposed amendments to the Standing Comm. *Id.* After approval by

today's complex electronic discovery procedures.[22] It is worthwhile to take a closer look at the rules' functions in order to determine how cloud computing service providers may fit into the overall procedural scheme.

Of vital importance to the 2006 Amendments, Rule 26(a)(1)(A) lays the groundwork for the practice of electronic discovery, stating that:

> [A] *party must without awaiting a discovery request, provide to other parties*: . . . (ii) a copy – or a description by category and location – of all documents, *electronically stored information*, and tangible things *that the disclosing party has in its possession, custody, or control* and may use to support its claims or defenses, unless the use would be solely for impeachment.[23]

Although electronically stored information may be voluntarily produced under Rule 26(a), a party may also obtain ESI in other ways. One of these ways for a party seeking ESI is to draft a motion to compel the discovery of ESI,[24] within the scope prescribed by Rule 26(b), on an opposing party.[25] For instance, the plaintiff in *Zubulake IV* filed a motion to compel the production of e-mails in a sex discrimination suit.[26] In order to compel production in this

---

the Standing Comm., the Judicial Conf. approved the proposed amendments on Sept. 20, 2005. JUDICIAL CONF. OF THE U.S., REP. OF THE PROCEEDINGS OF THE JUDICIAL CONF. OF THE U.S. 37 (2005). However, they are considered the 2006 amendments to the FRCP because that is the year they went into effect.

22. *See* Tanya L. Forsheit, *E-Discovery Involving Cloud Facilities*, 1010 PLI/PAT 157, 159–68 (2010).

23. FED. R. CIV. P. 26(a)(1)(A) (emphasis added).

24. FED. R. CIV. P. 34(a)(1)(A).

> A party may serve on any other party a request within the scope of Rule 26(b) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control: any designated documents or electronically stored information . . . stored in any medium from which information can be obtained either directly . . . .

Id.

25. FED. R. CIV. P. 26(b)(2)(B).

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.

Id.

26. *See, e.g.*, Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212,

manner, the moving party must specify the form of production for the ESI.[27] In the absence of such a stipulation or court order, with respect to the form of production, a producing party must produce ESI in the form in which it is ordinarily maintained or in a reasonably usable form.[28] In addition to the two mechanisms described above, a party may subpoena a non-party service provider to produce ESI pursuant to Rule 45.[29] For example, in *Flagg*, the plaintiff subpoenaed the defendant-city's text messaging provider for production of text messages concerning an alleged murder.[30]

Yet, there are two exceptions that may enable the court to deny a requesting party's motion to compel the production of ESI. ESI need not be produced in the two following situations: (1) if the ESI is not readily accessible due to undue burden or cost;[31] or (2) if the balance between the ESI's benefit and its evidentiary importance or production expense weighs against the moving party.[32] Rule 26 also grants the

215 (S.D.N.Y. 2003).

27. FED. R. CIV. P. 34(b)(1) ("The request must describe with reasonable particularity each item or category to be inspected; must specify a reasonable time, place, and manner for the inspection and for performing related acts; and may specify the form or forms in which electronically stored information is to be produced."); *see, e.g.*, Wyeth v. Impax Labs., Inc., 248 F.R.D. 169 (D. Del. 2006).

28. FED. R. CIV. P. 34(b)(2)(E).

> Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information: A party must produce documents as they are kept in the usual course of business . . . ; if a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms . . . .

Id.; *see, e.g.*, Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640 (D. Kan. 2005).

29. FED. R. CIV. P. 45(a)(1)(D) ("A command in a subpoena to produce a document, electronically stored information, or tangible things requires the responding party to permit inspection, copying, testing, or sampling of the materials.").

30. *See* Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

31. FED. R. CIV. P. 26(b)(2)(B).

32. FED. R. CIV. P. 26(b)(2)(C).

> On motion or on its own, the court must limit the frequency or extent of discovery . . . if it determines that . . . the burden of expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

Id.

trial court substantial latitude in deciding whether a discovery request constitutes an undue burden that would justify not producing the requested ESI.[33] Lastly, Rule 37 includes a safe harbor provision that may shield the non-moving party from the imposition of sanctions for failing to produce ESI, if the requested ESI has been lost as a result of the routine, good faith operation of an electronic information system.[34]

B. Application of the Zubulake IV *Framework to the Spoliation of ESI in the Cloud*

It is essentially Judge Scheindlin's opinion in *Zubulake IV* that created a framework for analyzing the spoliation of electronically stored information.[35] The Judiciary Committee borrowed heavily from Scheindlin's framework to draft the 2006 Amendments to the FRCP, which are discussed above.[36]

In *Zubulake IV*,[37] the plaintiff, a former equities trader for UBS, filed a complaint against UBS for gender discrimination for failure to promote and retaliation.[38] During the discovery process, the plaintiff requested e-mail correspondence sent between various UBS employees that were exclusively stored on UBS' proprietary computer systems.[39] Due to UBS' failure to preserve the e-mail correspondence, the plaintiff sought to impose discovery sanctions against UBS.[40] The court, in rendering its opinion, created an analytical framework for the party seeking to

33. Erin Marie Secord, *Exploring Challenges with the Discovery of Text Messages in Federal Cases Through the Lens of the Federal Rules of Civil Procedure and the Stored Communications Act*, 15 SUFFOLK J. TRIAL & APP. ADOV. 143, 146 (2010).

34. FED. R. CIV. P. 37(e) ("Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.").

35. *See* Cross & Kuwahara, *supra* note 8, at 9–10.

36. *See* Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information*, 58 S.C. L. REV. 7, 15 (2006) (maintaining that the "series of rulings by Judge Scheindlin in the Zubulake litigation have shaped the contours of electronic discovery and provide an example of how electronic discovery issues emerge within litigation").

37. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212 (S.D.N.Y. 2003).

38. *Id.*

39. *Id.* at 215.

40. *See id.*

impose sanctions for spoliation, or the deletion, of evidence.[41] The framework provides that the seeker must establish the following three elements, in order to prevail on such a motion:

> (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed;
>
> (2) that the records were destroyed with a culpable state of mind; and
>
> (3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense. [42]

In order to avoid falling victim to situations similar to UBS', a company contemplating entering into a contract, or currently in a contract, with a third-party cloud computing service provider should consider, and incorporate, safeguard provisions in their service contract as well as enact accompanying company policies to avoid sanctions for the spoliation, or deletion of ESI.

1. Mitigating Liability Under Prong I of the Zubulake IV *Framework*

Under the first element of the *Zubulake IV* analysis, a company should not fear the imposition of sanctions, unless "the party having control over the evidence had an obligation to preserve it at the time it was destroyed."[43] This element also implicates a series of secondary considerations, including (a) the date on which the duty to preserve is triggered, (b) the scope of the duty to preserve, which includes the key players in litigation and the lifeline of ESI, and (c) the format in which the ESI is to be produced. Finally, the party, upon which a production request is placed, must, in fact, (d) have necessary possession, custody, or control of the ESI.

i. Trigger Date for a Litigation Hold

Generally, "[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to the anticipated

41. *See id.* at 220.
42. *Id.*
43. *Id.*

litigation."[44] Other circuit courts, however, require more certainty as to whether litigation is likely before the duty to preserve arises, whereby "litigation must be probable rather than a [mere] possibility, and the path to litigation must be clear and immediate."[45] Yet, some circuit courts construe anticipation more broadly whereby the litigation hold is triggered when the defendant corporation retained counsel in connection with legal action but had yet to identify an allegedly responsible party.[46] In light of the uncertainty of the split among circuit courts apropos, the trigger of a litigation hold, the best practice and a "helpful analytical tool [for determining when the duty to preserve attaches] is the more widely developed standard for anticipation of litigation under the work product doctrine."[47] Work product doctrine protection attaches to documents "prepared *because* of the prospect of litigation when the preparer faces an actual or a potential claim following an actual event or series of events that reasonably could result in litigation."[48]

The simplest measure to prevent the imposition of sanctions is a company's ability to quickly put a litigation hold into place. The company needs to be able to implement a litigation hold on data retained by their third-party cloud computing service provider once they reasonably anticipate litigation,[49] subject to several small wrinkles in different

44. *Id.* at 216 n.13 (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1999)).

45. Hynix Semicond., Inc. v. Rambus, Inc., 591 F. Supp. 2d 1038, 1062 (N.D. Cal. 2006) (holding that litigation must be probable, rather than a possibility and the path to litigation must be clear and immediate before the duty to preserve arises); *see, e.g.*, Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 621 (D. Colo. 2007) (stating that "[w]hile a party shouldn't be permitted to destroy potential evidence after receiving unequivocal notice of impending litigation, the duty to preserve relevant documents should require more than a mere possibility of litigation."); Treppel v. Biovail Corp., 233 F.R.D. 363, 371 (S.D.N.Y. 2006) (stating that the mere existence of a dispute does not necessarily mean that parties should reasonably anticipate litigation or that the duty to preserve arises).

46. Innis Arden Golf Club v. Pitney Bowes, Inc., 257 F.R.D. 334, 340 (D. Conn. 2009).

47. Samsung Elecs. Co. v. Rambus, Inc., 439 F. Supp. 2d 524, 542 (E.D. Va. 2006).

48. *Id.* (citing Nat'l Union Fire Ins. Co.v. Murray Sheet Metal Co., 967 F.2d 980, 984 (4th Cir. 1992).

49. *See Samsung Elecs. Co.*, 439 F. Supp. 2d at 542. The best practice for determining the trigger date for a litigation hold should be the more widely developed standard for anticipation of litigation under the work product

circuits' jurisprudence.[50] This may be accomplished by contracting for the right, in a company's service agreement with a third-party cloud computing service provider, to stop the routine destruction of data at the discretion of the company's general counsel or officer. If ESI is preserved in the first instance, there is no need to advance to the second and third prongs of the *Zubulake IV* analysis because the last two prongs require ESI to be destroyed.

ii. Scope of the Duty to Preserve ESI

The duty to preserve ESI does not apply to every document a company has ever created, or will create. Instead, "[a] party or anticipated party must *retain all relevant documents* (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter."[51] For example, an e-mail correspondence drafted by a supervisor concerning an employee's performance review for a promotion in an employment discrimination case would be subject to the duty to preserve.[52] This, however, does not mean that a corporation, upon recognizing a threat of litigation, must preserve every shred of paper or every file of ESI, because such a stringent rule would serve to cripple large corporations that produce voluminous amounts of ESI and are frequently engaged involved in litigation.[53]

The duty to preserve is not so draconian; on the contrary, it extends only to "individuals likely to have discoverable information that the disclosing party may use to support its claims and defenses."[54] Thus, the duty covers persons "likely to have relevant information—the 'key players' in the case."[55]

The scope of discovery of the preservation duty is further restricted by the accessibility of the ESI in its current

doctrine.

50. *See generally supra* notes 45–46 and accompanying text.

51. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

52. *See* Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309, 312–13 (S.D.N.Y 2003); *see also* Bellinger v. Astrue, CV-06-321 (CBA), 2009 U.S. Dist. LEXIS 71727, at *2–3 (E.D.N.Y. Aug. 14, 2009).

53. *Zubulake IV*, 220 F.R.D. at 217.

54. *Id.* at 218.

55. *Id.*

condition.[56] In *Zubulake I*, five categories of data were described from the most to the least accessible:

> (1) Active, online data: data generally stored on magnetic disk that is used in the very active stages of an electronic record's life (e.g., data on hard drives);
>
> (2) Near-line data: data stored on a robotic storage device that houses removable media (e.g., optical disks);
>
> (3) Offline storage/archives: data on removable optical disk or magnetic tape media traditionally used for making disaster copies of records and also for records considered archival;
>
> (4) Backup tapes: a device, like a tape recorder, that reads data from and writes it onto a tape; and
>
> (5) Erased, fragmented or damaged data: as files are erased, their previous contiguous clusters are made available again as free space and the broken up files are randomly placed throughout the disk.[57]

Although this is a somewhat dated description of the categories within the lifeline of digital information, it still serves as a guidepost for the accessibility of ESI as it evolves from primary to archival data.[58] However, since it generally takes the law some time to catch up with and adapt to technology, the lifeline of ESI, as it shifts from a readily accessible active format to inaccessible data, presents a continuing challenge to the scope of the duty to preserve.[59]

Since the scope of the duty to preserve, triggered by anticipated or ongoing litigation, is determined largely upon who has accumulated and retained data in the cloud, it is imperative for a company to be able to quickly identify the relevant key players involved in the corresponding litigation when implementing a litigation hold. This objective may be realized if the company inserts flexibility into their service agreement with their third-party cloud computing service provider. Such flexibility would require the company to be able to easily access and place a non-deletion hold on a key player's ESI that is stored in the cloud by a simple search

56. Crist, *supra* note 36, at 30.
57. *Zubulake I*, 217 F.R.D. at 319.
58. *See* Crist, *supra* note 36, at 26.
59. *Id.*

function. The ability to identify key players in order to implement a litigation hold may be further achieved by integrating a clause into the service agreement, employment contracts, and company handbooks, that enables the company's general counsel, or specified officer, to exercise discretion over placing a litigation hold on any employee, considered a key player to the anticipated or ongoing litigation, and who has or continues to use of the service provider's cloud computing applications.

The scope of a key players' ESI that must be preserved includes "all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter."[60] A company's service agreement with their third-party cloud computing service provider must therefore articulate a certain amount of flexibility in order to effectuate the company's ability to retrieve the proper documents and to adapt to the corresponding suit they are engaged in because no two cases will require the same suite of ESI to be produced to a requesting party.

Compliance with the scope of the duty to preserve may also be achieved in a manner that is similar to selecting which employees' ESI to preserve. The company should contract for, in the service agreement with their third-party cloud computing service provider, the right to retrieve and preserve certain types of documents relevant to the anticipated or ongoing litigation in an easily searchable and definable manner. The service agreement should state that this right remains at the discretion of the company's general counsel, or a specified officer similarly equipped with the authority and competence to make such a determination.

iii. Format for the Production of ESI

A company that employs a third-party cloud computing service provider needs to be mindful of the format in which it may be compelled to produce ESI in future litigation when drafting its service agreement. Generally, a party that produces documents for inspection shall, pursuant to Rule 34, produce them as they are kept in the usual course of business or shall organize and label them to correspond with the

60. *Zubulake IV*, 220 F.R.D. at 218.

categories in the request.[61] Rule 34, in turn, raises issues such as whether the ESI should be produced with "metadata"—which is defined as data about the data[62]—and whether the ESI should be produced in its native file format or some other format.[63]

In determining whether metadata should be produced under a Rule 34 request, the court in *Williams v. Sprint/United Management Co.*[64] faced a question of first impression and looked to the Sedona Principles for guidance.[65] The party seeking ESI requested that spreadsheets be produced with their original metadata intact, instead of being produced in a TIFF image format.[66] The court agreed with the requesting party by reasoning that in light of emerging standards, "the producing party should produce the electronic documents with their metadata intact, unless the party timely objects to production of the metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."[67] The initial burden, with regard to disclosure of metadata, is thus placed on the producing party.[68]

---

61. FED. R. CIV. P. 34(b)(2)(E).

62. Adam K. Israel, *To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery*, 60 ALA. L. REV. 469, 469 (2009). "As a general rule of thumb, the more interactive the application, the more important the metadata is to understanding the application's output." Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 647 (D. Kan. 2005). The basic metadata characteristics can show whether a document has been inadvertently or intentionally modified, thereby performing a crucial function in establishing whether a document is genuine. *See* Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 12 (2007).

63. This will depend on both the Circuit the litigation is taking place and also whether the requesting party stipulates as to which file format the ESI should be produced. *See infra* notes 64, 69, 71 and accompanying text.

64. *Williams*, 230 F.R.D. at 652.

65. Comment 9.a of The Sedona Principles uses viewability as the determining factor in whether something should be presumptively treated as a part of a "document." *See* THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 30 (2003). Using viewability as the standard, all metadata ordinarily visible to the user of the Excel spreadsheet application should presumptively be treated as part of the "document" and should thus be discoverable. *See Williams*, 230 F.R.D. at 652.

66. *Williams*, 230 F.R.D. at 643.

67. *Id.* at 652.

68. *Id.*

Metadata was not discoverable in *Wyeth v. Impax Laboratories, Inc.*, because the court determined that the parties had never agreed that electronic documents would be produced in any particular format; therefore, Wyeth had complied with its discovery obligations by producing the ESI as TIFF image files.[69] Impax, furthermore, had not demonstrated a particularized need for the metadata.[70] On the other hand, requesting parties most likely prefer the production of metadata in its unadulterated form as opposed to TIFF image files because image files take significantly longer to sift through, as they are not ordinarily text searchable.

Contrary to *Impax Laboratories*, the court in In re *Verisign, Inc. Securities Litigation* resolved that the production of the TIFF image files alone was not sufficient to fulfill the production order, and the electronic version must include not only include metadata but must also be searchable.[71] Additionally, the court in *Hagenbush v. 3B6 Sistemi Elettronici Industriali* held that the party requesting production of documents was entitled to identical copies in the same form in which 3B6 USA kept them in the usual course of business.[72]

Generally, a company that produces ESI for inspection pursuant to Rule 34 must produce the ESI as it is kept in the usual course of business.[73] The company, however, should organize and label the ESI in accordance with the categories in the request for production, if the request so states.[74] This indicates that the company will usually have to produce, to the best of their ability, ESI in its native, unaltered format.

As case law appears to imply, the best practice for a company to ensure compliance with respect to the format of

69. Wyeth v. Impax Labs., Inc., 248 F.R.D. 169, 171 (D. Del. 2006).

70. *Id.*

71. *In re* Verisign, Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243, at *1 (N.D. Cal. Mar. 10, 2004) (requiring that the documents be in electronic format is not contrary to law but is supported by the Federal Rules).

72. Hagenbush v. 3B6 Sistemi Elettronici Industriali, No. 04 C 3109, 2006 WL 665005, at *2 (N.D. Ill. Mar. 8, 2006). After the plaintiff had complied with the defendant's request to visit their facility to designate which documents to be produced, the plaintiff is entitled not to TIFF image files of the documents requested but to identical electronic copies as viewed at the defendant's facility. *Id*. at *1–2.

73. FED. R. CIV. P. 34(b)(2)(E).

74. *Id.*

their produced data is to adhere to the viewability rule adopted by the *Williams* court. In abiding by this rule, the court maintained that all metadata that is ordinarily visible to the user of a spreadsheet application should presumptively be treated as part of the document and should, thus, be discoverable.[75] In light of the viewability rule, the company should include a provision in its service agreement to guarantee that their third-party cloud computing service provider will undertake the following prescriptive and prospective measures; preserve visible metadata on ESI, flag ESI containing metadata to facilitate future searches for ESI containing metadata, and refrain from scrubbing metadata away. Therein, once the company anticipates litigation, it can quickly determine which documents would require the additional production of metadata—provided that the metadata has been stored in the first instance, and that it is either visible or specifically requested.

Yet, to further complicate matters, data that is stored in random access memory (RAM) may also be subject to production due to Rule 34(a)'s intention that the scope of the production of documents be as broad as possible.[76] In *Columbia Pictures, Inc. v. Bunnell*, the court determined that defendants operating a torrent file search website must produce RAM to the plaintiff motion picture studio.[77] Rule 34(a)(1),[78] as amended in 2006, encompasses data stored in any medium from which information can be obtained and does not include a carve out for information written to a medium that stores information only temporarily, such as RAM.[79] Moreover, the advisory committee's notes to the 2006 amendments to the FRCP express that Rule 34(a)(1) "is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments."[80]

In the wake of *Bunnell*, a company must be prepared to not only produce metadata, but also RAM related to ESI

75. *See* Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan. 2005).

76. Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 447 (C.D. Cal. 2007).

77. *See id.* at 445–46.

78. FED. R. CIV. P. 34(a)(1).

79. *Columbia Pictures, Inc.*, 245 F.R.D. at 447.

80. Advisory Comm. on 2006 amendment to FED. R. CIV. P. 34(a)(1).

stored by their third-party cloud computing service provider if a requesting party specifies as such. It is therefore advisable that a company contracting with a third-party cloud computing service provider include provisions in their service agreement that specify for the continued maintenance and retention of both metadata and RAM for applicable files, especially after a litigation hold has been put in place. Otherwise, the company faces potential spoliation sanctions for the deletion of this desired data. With this protective provision serving as one of the terms of the service agreement, a company subjected to sanctions for spoliation of metadata and/or RAM, at the very least, may allege that the third-party cloud computing service provider committed a breach of contract in a subsequent claim against the offending provider.

iv. Control of ESI

A company that stores its data with a third-party cloud service provider need only produce ESI that is under the company's possession, custody, or control.[81] However, control of ESI does not require that the party have legal ownership or actual possession of the documents at issue.[82] Rather, documents may be considered to fall under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action.[83] This is particularly applicable when a company employs a third-party cloud computing service provider to store its data. In practice, courts have interpreted Rule 34 "to require production if the party has the *practical ability to obtain the documents* from another, irrespective of his legal entitlement to the documents."[84]

While the practical ability test, mentioned above, may be useful in assessing a party's obligations under Rule 34, the control test is more useful in determining the control required to trigger a party's duty to preserve evidence.[85] The control

81. *See* FED. R. CIV. P. 34(a)(1).

82. *See In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007).

83. *Id.*

84. Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 525 (S.D.N.Y. 1992) (emphasis added).

85. Goodman v. Praxair Services, Inc., 632 F. Supp. 2d 494, 516 n.11 (D. Md. 2009).

test was explicated by the court in In re *NTL, Inc. Securities Litigation*, which stated that the "test for production of documents is control, not location . . . where the documents are considered to be under a party's control when that party has the right, authority or practical ability to obtain the documents from a non-party to the action."[86]

Application of the control test to documents held by a third-party occurred in *Tomlinson v. El Paso Corp.*, whereby the plaintiff sought to compel the production of records from a company controlling a pension plan who in turn had retained a third-party to maintain the electronic records associated with the pension plan.[87] The company was under a duty to maintain certain records to comply with the Employee Retirement Income Security Act[88] and could not discharge this duty by having a third-party maintain its records.[89] Therefore, even though a third-party was maintaining the company's records, the court determined that the company was still in possession, custody, or control of the documents because they had or should have had the authority or ability to obtain the requested data from the third-party.[90]

Similarly, the court in *Flagg*[91] determined that the City of Detroit had sufficient control of ESI to permit production by its third-party service provider in the face of a subpoena.[92] Sufficient control existed because the City possessed the authority to consent to production of text messages stored by its third-party service provider, SkyTel, in relation to the alleged murder of the plaintiff's mother.[93] The City of Detroit entered into a contract with SkyTel to provide the municipality with text messaging devices and corresponding services for various city officials.[94] Because the City had the ability to grant its consent to their third-party service provider to obtain the records, it was considered to be in

86. *In re NTL, Inc.*, 244 F.R.D. at 195.

87. Tomlinson v. El Paso Corp., 245 F.R.D. 474, 476–77 (D. Colo. 2007).

88. *See* 29 U.S.C. § 1059(a)(1) (2010). Under the Employee Retirement Income Security Act, an employer has the responsibility of the proper maintenance and retention of employees' pension and welfare plan records.

89. *See Tomlinson*, 245 F.R.D. at 477.

90. *Id.*

91. Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008).

92. *Id.* at 354.

93. *Id.*

94. *Id.* at 347.

control of the ESI, and the City could not simply refuse to give consent and maintain that the records were out of their control in a Rule 34 context.[95] The court in *Flagg* proceeded with its analysis under the assumption that the request for production of the text messages came under a Rule 34 motion to compel.[96] The court thereby required the plaintiff to reformulate its discovery request from a Rule 45 subpoena[97] of SkyTel to a Rule 34 motion to compel[98] upon the City of Detroit to avoid complications under the Electronic Communications Privacy Act (ECPA).[99]

Dietrich v. Bauer[100] exemplified another instance in which a party to litigation was determined to be in control of information that was maintained by a third-party. In this case, a parent company exercised sufficient control over the documents of its subsidiary to render it responsible for producing the requested documents.[101] Likewise, those who engage in joint ventures have a legal right to obtain information from his or her fellow venturer upon demand for production of documents.[102] With respect to data held by a former employee, the court in *Export-Import Bank of the United States v. Asia Pulp & Paper Co.*[103] found that the plaintiff-bank fulfilled the control test, because it had the apparent practical ability to obtain requested documents from its non-party former employee.[104] Alternatively, at the very least, the bank was compelled to ask its former employee for the documents before asserting that it had no control over the documents in the former employee's possession.[105]

95. *Id.* at 355.
96. *Id.* at 366.
97. FED. R. CIV. P. 34(a)(1)(A).
98. FED. R. CIV. P. 45(a)(1)(D).
99. *Flagg*, 252 F.R.D. at 366. The court determined that it was unclear whether under the ECPA SkyTel's records would be protected and not be subject to a Rule 45 subpoena for records. *See id.*
100. Dietrich v. Bauer, 95 Civ. 7051 (RWS), 2000 U.S. Dist. LEXIS 11729 (S.D.N.Y. Aug. 16, 2000).
101. *Id.* at *9.
102. Starlight Int'l, Inc. v. Herlihy, 186 F.R.D. 626, 635 (D. Kan. 1999) (stating that joint venturers have the right, authority or practical ability to produce documents that are held by a member of the joint venture because a joint venture is treated as a partnership in Kansas).
103. Exp.-Imp. Bank of the U.S. v. Asia Pulp & Paper, 233 F.R.D. 338 (S.D.N.Y. 2005).
104. *Id.* at 341.
105. *Id.*

Further, the court in *Tetra Technologies, Inc. v. Hamilton* found that the defendant, a subscriber/user of a cell phone service, had sufficient control over his personal cell phone records to be obligated to produce them in the face of a Rule 34 motion to compel. The defendant fulfilled the control test, because he possessed the legal right to obtain the phone records, which were requested by the plaintiff.[106] Again, in *Cyntegra, Inc. v. Idexx Laboratories, Inc*., the court found that the defendant-company satisfied the control test and consequently sanctioned the company for failing to make payments to its third-party data storage company, who in turn deleted the discoverable data from its servers as a result of this non-payment.[107]

As the cases above explicate, a company that employs a third-party cloud computing service provider to retain data will be deemed by a court to be in control of the data maintained by the service provider for production and preservation purposes.[108] Even though the ESI is not within the company's possession, the ESI is still within the company's control, because the company has the legal right to obtain it.[109]

Few courts have commented specifically on discovery obligations within the context of cloud computing,[110] but situations in which possession and control are similarly split between a party to the litigation and a third-party service provider, provide helpful analogies.[111] Although the company has legal control of the ESI in the eyes of the court, the third-party cloud computing service provider may refuse to retrieve the ESI in the proper format; respecting that the company needs to produce the ESI in the explicit and precise format in

106. Tetra Techs., Inc. v. Hamilton, No. CIV-07-1186-M, 2008 WL 3307150, at *1 (W.D. Okla. Aug. 7, 2008).

107. Cyntegra, Inc. v. Idexx Labs., Inc., No. CV 06-4170 PSG (CTx), 2007 WL 5193736, at *6–7 (C.D. Cal. Sept. 21, 2007).

108. *See* Flagg v. City of Detroit, 252 F.R.D. 346, 354 (E.D. Mich. 2008); *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007); Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007).

109. *See generally supra* note 95 and accompanying text.

110. Similarly, few courts have even mentioned cloud computing in there opinions except for one. *See* Oregon v. Beller, 217 P.3d 1094, 1111 n.11 (Or. Ct. App. 2009) (Sercombe, J., dissenting).

111. Charles B. Molster III & Elizabeth H. Erickson, *"Cloud Computing" in Discovery: How We Deal with Electronically Stored Information*, 59 VA. LAW. 60, 60 n.1 (2010).

order to comply with the opposing party's discovery request.

A company may avoid the problems brought by the lack of guidance regarding discovery obligations and cloud computing by adding a stipulation in its service contract with the third-party cloud computing service provider. The contract term may allow the company, at the discretion of the company's general counsel or a specified officer, to obtain ESI in the event of anticipated litigation within a specified window of time. Whether non-parties to litigation—such as third-party cloud computing service providers—may hide behind the shield of the ECPA when subpoenaed by the opposing party to produce ESI is still unclear.[112]

2. Mitigating Liability Under Prong II of the Zubulake IV *Framework*

The second element of the *Zubulake IV* framework requires that a party to destroy evidence with a culpable state of mind in order for the imposition of sanctions for the violation of the duty to preserve.[113] A company employing a third-party cloud computing service provider may address the culpability requirement by being proactive when drafting the service agreement and tailoring it to the applicable jurisdiction's case law so that both parties acknowledge and are informed of the relevant culpability standard. Potential sanctions on a scale of most to least severe include: dismissal of a claim or granting judgment in favor of a prejudiced party, suppression of evidence, an adverse inference, fines, and attorneys' fees and costs.[114]

Even though federal law governs the instant sanctioning process for spoliation of evidence, as the sanctions constitute evidentiary matters,[115] the extent of culpability required to incur sanctions varies from circuit to circuit. The range of culpability for destruction of ESI includes bad faith, gross

112. *See Flagg*, 252 F.R.D. at 366.

113. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 220 (S.D.N.Y. 2003). The level of culpability is of prime importance in the court's determination of the appropriate sanction. *See* Crist, *supra* note 36, at 45.

114. Mosaid Techs., Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 335 (D.N.J. 2004).

115. Se. Mech. Serv., Inc. v. Brody, No.: 8:08-CV-1151-T-30EAJ, 2009 U.S. Dist. LEXIS 69830, at *6 (M.D. Fla. July 24, 2009) (citing Flury v. Daimler Chrysler Corp., 427 F.3d 939, 944 (11th Cir. 2005)).

negligence, and ordinary negligence.[116] Yet, once the duty to preserve attaches to discoverable ESI, "any destruction of documents is, at a minimum, negligent."[117] When a party seeks a sanction that would terminate litigation, such as a request for dismissal or default judgment, the circuits uniformly require a showing of bad faith.[118] An adverse inference is an instruction to the jury that there is a rebuttable presumption that the lost evidence is both relevant and favorable to the questing party's claims or defenses.[119] The showing of culpability required for an adverse inference instruction varies by circuit court.[120]

A reflection of the fragmentation among the circuit courts begins with the lowest level of culpability necessary for the imposition of sanctions, whereby a court, within the Second Circuit, in *Pension Comm. of the University of Montreal v. Banc of America Securities, LLC*, imposed an adverse inference after finding that the defendant had destroyed ESI in a manner amounting to gross negligence.[121] The Second Circuit further allows for the imposition of an adverse inference based on negligent destruction alone.[122] In the First, Fourth, and Ninth Circuits, bad faith is not essential for imposing an adverse inference as long as there is severe prejudice—although the presence of bad faith is often emphasized.[123] The Seventh, Eighth, Tenth, and D.C.

116. *See* Cross & Kuwahara, *supra* note 8, at 11 n.52.

117. *Zubulake IV*, 220 F.R.D. at 220.

118. Crist, *supra* note 36, at 45.

119. Pension Comm. of Montreal Univ. v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 470 (S.D.N.Y. 2010).

120. *See* Cross & Kuwahara, *supra* note 8, at 11 n.59.

121. *See Pension Comm. of Montreal Univ.*, 685 F. Supp. 2d at 470.

122. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (stating that "[t]he sanction of an adverse inference may be appropriate in some cases involving negligent destruction of evidence because each party should bear the risk of its own negligence").

123. *See, e.g.*, Silvestri v. Gen. Motors Corp., 271 F.3d 583, 593 (4th Cir. 2001) (holding that dismissal is usually justified only in circumstances of bad faith but even where conduct is less culpable, dismissal may be necessary if the prejudice to the other party is extraordinary); Sacramona v. Bridgestone/Firestone, Inc., 106 F.3d 444, 447 (1st Cir. 1997) ("Certainly bad faith is a proper and important consideration in deciding whether and how to sanction conduct resulting in the destruction of evidence. But bad faith is not essential."); Glover v. BIC Corp., 6 F.3d 1318, 1329 (9th Cir. 1993) (stating that a trial court has broad discretionary power to permit a jury to draw an adverse inference from the spoliation against the party responsible for such behavior).

Circuits impose an adverse inference only after finding bad faith.[124] Likewise, in *Rimkus Consulting Group v. Cammarata*, a decision rendered within the Eleventh Circuit, the court required a showing of bad faith to impose an adverse inference.[125] The Third Circuit follows a more unique approach by balancing the degrees of fault and prejudice to determine the culpability of the spoliating party and the appropriate sanctions.[126]

Regardless of the level of culpability that applies, an enterprise employing a cloud computing service provider has a safe harbor from the imposition of sanctions. An enterprise may employ this safe harbor, under Rule 37(e), if their cloud computing service provider routinely destroys data in "good-faith."[127] More specifically, under Rule 37(e), sanctions are inappropriate (1) where electronic communications are destroyed pursuant to a computer system's routine operations, and (2) where there is no evidence that the system was operated in bad faith.[128] Regardless, once litigation is anticipated, as discussed in Part I.B.1.i, the company certainly should instruct its third-party cloud computing service provider to disable all routine destruction policies and place a litigation hold on their relevant ESI.[129]

---

124. *See, e.g.*, Turner v. Pub. Serv. Co. of Colo., 563 F.3d 1136, 1149 (10th Cir. 2009) ("Mere negligence in losing or destroying records is not enough . . . .") (quoting Aramburu v. Boeing Co., 112 F.3d 1398, 1407 (10th Cir. 1997)); Faas v. Sears, Roebuck & Co., 532 F.3d 633, 644 (7th Cir. 2008) (stating that in order to draw an adverse inference, "we must find that Sears intentionally destroyed the documents in bad faith."); Greyhound Lines, Inc. v. Wade, 485 F.3d 1032, 1035 (8th Cir. 2007) (holding that a spoliation of evidence sanction requires a finding of intentional destruction).

125. Rimkus Consulting Grp. v. Cammarata, 688 F. Supp. 2d 598, 614 (S.D. Tex. 2010). The Eleventh Circuit also requires bad faith for an adverse inference. *See* Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1294 (11th Cir. 2003) ("[A]n adverse inference is drawn from a party's failure to preserve evidence only when the absence of that evidence is predicated on bad faith.") (quoting Bashir v. Amtrak, 119 F.3d 929, 931 (11th Cir. 1997)).

126. *See* Mosaid Techs., Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (noting that "three key considerations dictate whether sanctions are warranted: (1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness . . .").

127. *See* FED. R. CIV. P. 37(e).

128. Se. Mech. Serv., Inc. v. Brody, No.: 8:08-CV-1151-T-30EAJ, 2009 U.S. Dist. LEXIS 69830, at *13 (M.D. Fla. July 24, 2009).

129. *See, e.g.*, Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007) (imposing sanctions for failure to turn off an automatic deletion feature once informed of

As discussed earlier, the level of culpability that will warrant the imposition of sanctions varies among the circuit courts, especially for the imposition of an adverse inference. Still, once the duty to preserve attaches, "any destruction of documents is, at a minimum, negligent."[130] Therefore, an enterprise employing a third-party cloud computing service provider must draft their service agreement in such a fashion, where once a litigation hold is triggered the routine destruction of ESI is immediately disabled. The enterprise should also make reasonable efforts to become knowledgeable and stay informed of which circuit's culpability jurisprudence is applicable when drafting their service agreement.

More specifically, it is strongly advised that the enterprise negotiate in an indemnity provision commensurate with the most current case law in the jurisdiction that applies to the service agreement. The indemnity provision should include some flexibility that anticipates the possibility for case law in the corresponding jurisdiction to become stricter with regards to their interpretation of the second element of the *Zubulake IV* framework.

3. Mitigating Liability Under Prong III of the Zubulake IV *Framework*

The third and final element of the *Zubulake IV* framework requires that "the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense" before sanctions may be imposed by the court for failure to preserve ESI.[131] "Relevant" in this context is defined as something more than sufficiently probative[132] to

pending litigation without finding bad faith); Broccoli v. Echostar Commc'n Corp., 229 F.R.D. 506, 511–12 (D. Md. 2005) (finding that Echostar had engaged in gross spoliation because it had failed to suspend its email and data destruction policy once litigation was reasonably anticipated); Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264, 282 (E.D. Va. 2004) ("[O]nce a party reasonably anticipates litigation, it has a duty to suspend any routine document purging system that might be in effect and to put in place a litigation hold to ensure the preservation of relevant document—failure to do so constitutes spoliation.").

130. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 220 (S.D.N.Y. 2003).

131. *Id.*

132. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002).

satisfy Rule 401 of the Federal Rules of Evidence.[133] If ESI is destroyed in bad faith, either intentionally or willfully, this fact alone is enough to establish relevance.[134] In the absence of bad faith, however, this element must be established by the submission of extrinsic evidence demonstrating the absent evidence would have been favorable to the party seeking sanctions.[135]

In terms of approaching this third prong, the best practice for a company anticipating litigation is to produce ESI that is relevant within the context of Rule 401 of the Federal Rules of Evidence, whereby the ESI must be more than sufficiently probative.[136] If ESI does not meet the Rule 401 threshold, the company should use its best judgment in withholding the ESI. If the ESI is not destroyed in bad faith, the third prong of the *Zubulake IV* framework appears to be more preferential to the producing party rather than the requesting party, or the party seeking to impose sanctions, as it places a fairly heightened burden of proof upon the latter to locate and provide extrinsic evidence with a tendency to show that the missing evidence would have been favorable to its position.

III. PROACTIVE MEASURES TO LESSEN THE RISK OF SANCTIONS FOR SPOLIATION OF ESI

In today's business environment, companies are outsourcing more of their data services, both data storage and processing, which is leading to the emergence and rapid adoption of cloud computing solutions that entail third-party administration and control of basic technology services.[137] In light of this new method of storing ESI, companies must make additional efforts to reduce the risk of court sanctions and liability by drafting advantageous provisions in service agreements with a third-party cloud computing service provider in contemplation of prospective litigation and lack of

133. FED. R. EVID. 401.

134. *Zubulake IV*, 220 F.R.D. at 220.

135. Chan v. Triple 8 Palace, Inc., 03 Civ. 6048 (GEL) (JCF), 2005 U.S. Dist. LEXIS 16520, at *23 (S.D.N.Y. Aug. 11, 2005).

136. *Residential Funding Corp.*, 306 F.3d at 108.

137. *See* Renee T. Lawson, *Cloud Computing and IT Outsourcing - Unforeseen Hiccups for E-Discovery in the Wake of Quon v. Arch Wireless?*, 832 PLI/LIT 203, 212–13 (2010).

cooperation by the service provider. A company may be subject to liability if its third-party cloud computing service provider's actions relating to the company's ESI, which includes their non-compliance with a request to produce ESI because, as case law has demonstrated (e.g., the commonly used control test from In re *NTL, Inc.*) the company holds control over its ESI even if the company does not have possession of the ESI.[138] The company therefore needs to implement a provision in the service agreement with its third-party cloud computing service provider, which enables one of the company's agents, such as the general counsel or a specified corporate officer, to demand that ESI be handed over to the company within a short period of time.

The company must also have the ability to quickly place a litigation hold on specified relevant ESI, and to direct its third-party service provider to disable routine deletion procedures to stave off spoliation sanctions. Further, in the event of a Rule 34 request for ESI, provisions must be incorporated into the service agreement whereby the cloud computing service provider can produce metadata and, also, RAM, if necessary. A contractual provision should additionally be added to the company's service agreement, whereby, in the event that the third-party cloud computing service provider is subpoenaed, the company's counsel will receive a notice of all subpoenas that concern the company's ESI as well as a right of first refusal over the service provider's production of the company's ESI.

The service agreement should also address which party incurs liability for sanctions stemming from any spoliation of the company's ESI. An indemnification clause in the service agreement could provide indemnification for the company from the third-party cloud computing service provider for all sanctions resulting from the service provider's destruction of relevant ESI after the company has put a litigation hold on such relevant ESI. In addition to contractual provisions, the company should apprise the judge in a Rule 26 discovery conference that the company's relevant ESI will need to be obtained from its third-party cloud computing service provider. In doing so, the judge will be able to take into account the additional complications inherent in first

138. *See In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007).

obtaining ESI from a third-party for production in the discovery plan and also be subject to the court's order.

Finally, an enterprise engaged in litigation should consider the creation of a private network on the contracted third-party cloud computing service provider's system. Such a system would allow an opposing/moving party to directly access the requested ESI. Not only would such a system facilitate the requesting party's access for the requested ESI in its native format, it would also enable the producing party to restrict access exclusively within the bounds of discovery. Such a mechanism benefits both the requesting and producing parties: on the one hand, it would allow the requesting party access to what they precisely seek and, on the other, reassure the producing party that the ESI produced is only the ESI responsive to the discovery request and nothing more is at risk of being inadvertently disclosed.

CONCLUSION

As the shift towards the usage of third-party cloud computing service providers continues to grow, a company employing these services must adjust to the many facets and challenges that electronic discovery will potentially pose. A company itself holds the burden of drafting a service agreement that provides protection from liability for the spoliation of ESI by third-party cloud computing service providers. Sanctions for the spoliation of ESI are costly and can be crippling to litigation, as described *supra* with reference to adverse inferences.[139] To prevent this foreseeable consequence, it is strongly recommended that a company—in drafting their third-party cloud computing service agreement—integrate provisions that call for the implementation of litigation holds ceasing routine spoliation procedures when the enterprise anticipates litigation. Provisions that clearly establish whose ESI will be retained, the scope of ESI to be retained, in what form, and how it will be retained are also helpful in providing clear delineations of liability. By taking the proactive steps discussed in this Comment towards insulating itself from potential discovery

139. *See* Mosaid Techs., Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (explicating potential sanctions on a continuum of most to least severe); *infra* Part I.B.2.

sanctions, a company may more comfortably allow its data to "enter the cloud."